



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10255121 A**(43) Date of publication of application: **25 . 09 . 98**

(51) Int. Cl.

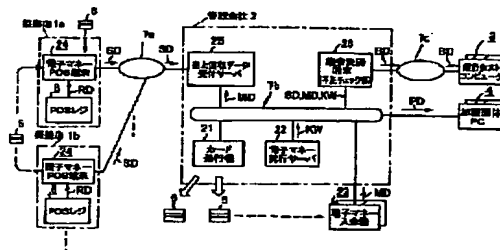
G07F 7/12
G06F 17/60
G06K 17/00

(21) Application number: **09055239**(22) Date of filing: **10 . 03 . 97**(71) Applicant: **GLORY LTD**(72) Inventor: **KAMISE YOUJIROU****(54) ELECTRONIC MONEY SYSTEM****(57) Abstract:**

PROBLEM TO BE SOLVED: To detect dishonesty such as the forgery/alteration of a card in a money payment process or the alteration of sales data in a store, and to ensure security by checking dishonesty from sales data and the data of an electronic money issuing device or the like, totaling a payment sum to the store, and transmitting it to the computer of a bank for a payment processing.

SOLUTION: An electronic money issuing server 22 stores/manages data such as security information KW such as the password of a card owner. A sales collection data accepting server 25 receives and stores money data MD paid to a pre-paid card 5 by an electronic money paying machine 23 and sales data SD stored in an electronic money POS terminal. A total settling terminal 26 checks the alternation of data based on the security information KW, sales data SD, and money data MD, totals a payment sum to the store, and transmits transfer data BD to a bank host computer 3 for a payment processing.

COPYRIGHT: (C)1998,JPO



特開平10-255121

(43)公開日 平成10年(1998)9月25日

(51) Int.Cl.⁸

識別記号

FI

G 0 7 F 7/12

G O 7 F 7/08

C

G O 6 F 17/60

G O 6 K 17/00

L

G 0 6 K 17/00

G 0 6 F 15/21

3 4 0 A

審査請求 未請求 請求項の数 3 O.L (全 12 頁)

(21)出願番号 特願平9-55239

(22)出願日 平成9年(1997)3月10日

(71)出願人 000001432

グローリー工業株式会社

兵庫県姫路市下手野1丁目3番1号

(72)発明者 神瀬 陽二郎

兵庫県姫路市下手野一丁目3番1号 グローリー工業株式会社内

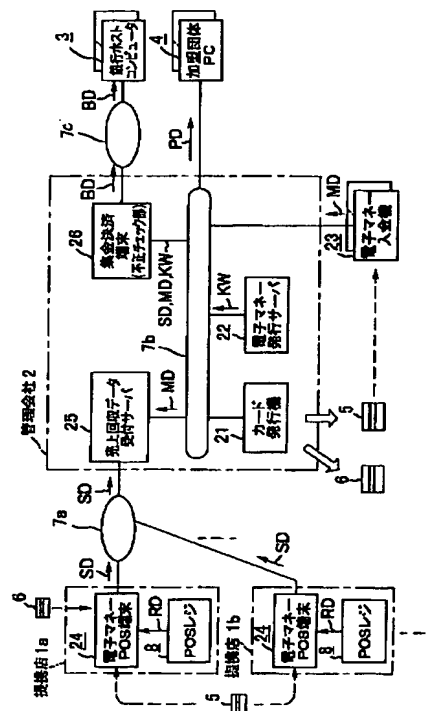
(74)代理人 弁理士 安形 雄三

(54)【発明の名称】 電子マネーシステム

(57) 【要約】

【課題】 金銭的価値を記憶させたカードによる金銭支払いの課程に於ける様々な不正を検出し、セキュリティを確保することができる電子マネーシステムを提供する。

【解決手段】 ICカード5に金銭的価値を記憶させると共に、発行の番号を付して発行する電子マネー発行装置21、23と、商品の購入の際に前記ICカードによる支払い処理を行うための電子マネーPOS端末24と、前記電子マネー発行装置のデータを記憶し管理するカード発行サーバ手段22と、前記電子マネーPOS端末から回線を通じて情報の供与を受ける売上回収データ受付サーバ手段25と、前記回収データ受付サーバ手段の記憶している売上データと前記カード発行サーバ手段のデータと前記電子マネー発行装置のデータとから不正のチェックをした後、該当店舗の支払い金額を集計して銀行のコンピュータ3に送信し実支払い処理を行う集計決済コンピュータ26とを備える。



【特許請求の範囲】

【請求項1】 現金若しくは後払い契約によりICカードに金銭的価値を記憶させると共に、購入者が使用する際の暗証番号を受付けると共に発行の番号を付して前記ICカードに記憶させて発行する電子マネー発行装置と、商品の販売店若しくはサービスの提供場所に設けられ、商品の購入の際に前記ICカードによる支払い処理を行うための電子マネーPOS端末と、前記電子マネー発行装置のデータを記憶し管理するカード発行サーバ手段と、前記電子マネーPOS端末から回線を通じて情報の供与を受ける売上回収データ受付サーバ手段と、前記回収データ受付サーバ手段の記憶している売上データと前記カード発行サーバ手段のデータと前記電子マネー発行装置のデータとから不正のチェックをした後、該店舗の支払い金額を集計して銀行のコンピュータに送信し支払い処理を行う集計決済コンピュータとを備えたことを特徴とする電子マネーシステム。

【請求項2】 利用者ICカードを受付けて内部に記憶されているパスワードを讀出すと共にプリペイド金額を讀出し更新するICカードリードライタと、少なくとも販売金額を入力するための売上金額入力手段と、利用者が暗証番号を入力するための暗証番号入力手段と、ガイダンス及び入力した金額を表示するための表示手段と、所定期間の売上データを記憶する記憶手段と、前記利用者ICカードを讀出した際には、該カード内部に記憶されている暗証番号と前記暗証番号入力手段より入力された利用者の暗証番号とが一致した場合に前記プリペイド金額を更新すると共に、該カード内部に記憶されている暗号キーによって利用者の支払いデータを暗号化して、同一情報で暗号化しないものを回収データとして前記暗号化されたデータとともに前記記憶手段に記憶し、店所有のICカードを讀出した際には、前記記憶手段に記憶されている回収データを該店所有のICカードの暗号化プログラムによって暗号化し、2種類の暗号化データを前記売上データとして所定期間分前記記憶手段に記憶させ、ホストコンピュータに電話を掛けて前記売上データを転送する制御部とを有する電子マネーPOS端末を具備したことを特徴とする電子マネーシステム。

【請求項3】 利用者により入力されたICマネーカードの暗証番号によりカード所持者の個人認証を行う第1の認証手段と、前記ICマネーカードに記録された暗号化プログラム及び第1の暗号キーにより利用金額を暗号化する第1の暗号化手段と、店舗担当者により入力された店舗用カードの暗証番号により取扱担当者の認証を行う第2の認証手段と、前記店舗用カードに記録された暗号化プログラム及び第2の暗号キーにより前記利用金額に対する売上金額を暗号化する第2の暗号化手段と、前記第1及び第2の暗号化手段によりそれぞれ暗号化された前記利用金額と売上金額の一对の暗号化データを纏めて送信する送信手段とを有する電子マネーPOS端末

と；前記電子マネーPOS端末からの前記一对の暗号化データを予め登録された第1及び第2の解除キーを用いてそれぞれ復号して両データの一致を確認すると共に、前記ICマネーカードの金銭的価値データを書換える電子マネー入金機からの入金金額データ及び前記復号された利用金額データに基づき、前記ICマネーカードに対する入金と出金との大小関係を比較して入出金の正当性を確認する不正検出手段を有する管理コンピュータと；を備えたことを特徴とする電子マネーシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカードをプリペイドカードとして使用した電子マネーシステムに関し、特に、金銭的価値を記憶させたカードによる金銭支払いの課程に於ける各種のデータ改ざんを検出し、セキュリティを確保し得るようにした電子マネーシステムに関する。

【0002】

【従来の技術】現在、カードを用いて商品の購入や各種サービスの利用をできるようにしたキャッシュレス・システムとしては、プリペイドカード・システム、クレジットカード・システム、銀行POSシステムといった様々なシステムが普及しており、近年では、いわゆる電子マネーによる取引を可能とした電子マネーシステムが実現されつつある。これらのキャッシュレス・システムでは、利用者が商品を購入してから決済が完了するまでの過程において様々な不正行為がなされる可能性がある。そこで、金銭的価値データを記録する媒体として磁気カードなどの媒体に比べて安全性の高いICカードを用いるようにしたシステムが数多く開発されている。

【0003】ICカードを用いたプリペイドカード・システムとしては、例えば特開平4-313190号公報に開示されている。このシステムは、銀行（銀行センターシステム）、利用者（ICカード）、及び店舗（取引端末）とでプリペイドカードシステムを構成しており、ICカードによる買物が行われるごとに、買物金額を加算して売上合算を計算し、そのデータを取引端末若しくはICカードに格納してある銀行鍵を使用して暗号化し、売上合算データとその暗号文を取引端末に格納する。そして、次回からは売上合算を算出する際に前回の売上合算データを暗号化して暗号文と比較、或いは暗号文を復号して売上合算データと比較し、データの改ざんがないか否かを判定する。そして、銀行センターシステムでは、取引端末から一定期間毎に送られてくる決済要求に対して取引端末と同一のロジックで売上合算データと暗号文とを照合し、一致していれば不正改ざんがないと判断して決済処理を実施するようになっている。しかしながら、この場合は店側でデータを暗号しているの

で、店側で売上データを改ざんすることが可能である。

【0004】一方、銀行とは異なる機関において、IC

カードをプリペイドカードとして際の代金の精算業務を行うようにしたシステムとしては、例えば特開平5-324998号公報に記載のものが挙げられる。このシステムは、加盟店共通の事務局（ホストコンピュータ）を設け、顧客に配布したICカードとのやりとりを行うことができるリーダ／ライタ装置を各加盟店に配置し、リーダ／ライタ装置とホストコンピュータとの間で情報の伝達を行い、代金の精算を集中管理するようにしたものである。このシステムにおいては、各顧客は事務局において住所や氏名を登録し、所定のプリペイド額を支払ってICカードを受取り、代金精算は加盟店からの取引情報がホストコンピュータに送られてきた取引情報に基づき行われる。また、顧客のICカードにはプリペイド残額の他に、売掛金残額やサービスポイント残額が記録されるようになっており、売掛金計上による支払いやサービスポイントからの支払いを可能としている。しかしながら、当公報には、セキュリティに関する技術内容に関する記載は何もない。

【0005】また、ICカードをプリペイドカードとして用い、プリペイドカードの残金を更新することで再利用できるようにしたシステムとしては、例えば特開平3-266095号公報に記載のものが挙げられる。この実施例に記載のキャッシュレスシステムは、銀行のホストコンピュータに接続されるプリペイド記録機と、銀行のホストコンピュータに接続される管理会社のコンピュータと、各店舗内に配置される専用端末とから構成される。そして、暗証番号を入れることにより読み書きが可能となるICカードを使用して、銀行のホストコンピュータに接続して暗証番号を入力してOKであれば自分の銀行口座から管理会社への振替金額であるプリペイド金額をICカードに書き込む。店でカードを使う際には、カードを専用端末に装着して暗証番号を入れた後に利用金額分を減算してカードのプリペイド金額を減算する。また、専用端末はカードが装填されたときには、管理会社のコンピュータと接続されていて所定期間毎に利用金額と店舗を示す情報を出力する様にしている。

【0006】

【発明が解決しようとする課題】 上述した従来のシステムでは、一般的な暗証番号による個人認証や銀行鍵を用いてデータ照合を行っていることが一部の公報に開示されている。しかしながら、データの改ざんに対する保証については詳しい記載がなく、店側とかデータの伝送時の安全保護については何も対策が講じられていない。企業内等の使用場所が限られたエリア内で適用する場合には、従来のシステムにおいても比較的セキュリティが確保されると言えるが、一般の店舗などにも利用範囲を拡張して適用する場合には、暗号等が解読されて一部のセキュリティが破れても、その不正を検出して取引を中止させることができるような、より安全性をきわめたシステムを構築して提供することが重要な課題と言える。

【0007】本発明は上述のような事情から成されたものであり、本発明の目的は、金銭的価値を記憶させたマネーカードによる金銭支払いの課程に於ける、カードの偽造／変造、店舗内における売上データの改ざん、伝送時のデータの改ざんなどの不正を検出し、セキュリティを確保することができる電子マネーシステムを提供することにある。

【0008】

【課題を解決するための手段】 本発明は、ICカードをプリペイドカードとして使用した電子マネーシステムに関するものであり、本発明の上記目的は、現金若しくは後払い契約によりICカードに金銭的価値を記憶させると共に、購入者が使用する際の暗証番号を受付けると共に発行の番号を付して前記ICカードに記憶させて発行する電子マネー発行装置と、商品の販売店若しくはサービスの提供場所に設けられ、商品の購入の際に前記ICカードによる支払い処理を行うための電子マネーPOS端末と、前記電子マネー発行装置のデータを記憶し管理するカード発行サーバ手段と、前記電子マネーPOS端末から回線を通じて情報の供与を受ける売上回収データ受付サーバ手段と、前記回収データ受付サーバ手段の記憶している売上データと前記カード発行サーバ手段のデータと前記電子マネー発行装置のデータとから不正のチェックをした後、該当店舗の支払い金額を集計して銀行のコンピュータに送信し支払い処理を行う集計決済コンピュータとを備えることによって達成される。

【0009】或いは、利用者ICカードを受付けて内部に記憶されているパスワードを読出すと共にプリペイド金額を読出し更新するICカードリードライトと、少なくとも販売金額を入力するための売上金額入力手段と、利用者が暗証番号を入力するための暗証番号入力手段と、ガイダンス及び入力した金額を表示するための表示手段と、所定期間の売上データを記憶する記憶手段と、前記利用者ICカードを読出した際には、該カード内部に記憶されている暗証番号と前記暗証番号入力手段より入力された利用者の暗証番号とが一致した場合に前記プリペイド金額を更新すると共に、該カード内部に記憶されている暗号キーによって利用者の支払いデータを暗号化して、同一情報で暗号化しないものを回収データとして前記暗号化されたデータとともに前記記憶手段に記憶し、店所有のICカードを読出した際には、前記記憶手段に記憶されている回収データを該店所有のICカードの暗号化プログラムによって暗号化し、2種類の暗号化データを前記売上データとして所定期間分前記記憶手段に記憶させ、ホストコンピュータに電話を掛けて前記売上データを転送する制御部とを有する電子マネーPOS端末を具備することによって達成される。

【0010】或いは、利用者により入力されたICマネーカードの暗証番号によりカード所持者の個人認証を行う第1の認証手段と、前記ICマネーカードに記録され

た暗号化プログラム及び第1の暗号キーにより利用金額を暗号化する第1の暗号化手段と、店舗担当者により入力された店舗用カードの暗証番号により取扱担当者の認証を行う第2の認証手段と、前記店舗用カードに記録された暗号化プログラム及び第2の暗号キーにより前記利用金額に対する売上金額を暗号化する第2の暗号化手段と、前記第1及び第2の暗号化手段によりそれぞれ暗号化された前記利用金額と売上金額の一对の暗号化データを纏めて送信する送信手段とを有する電子マネーPOS端末と；前記電子マネーPOS端末からの前記一对の暗号化データを予め登録された第1及び第2の解除キーを用いてそれぞれ復号して両データの一致を確認すると共に、前記ICマネーカードの金銭的価値データを書換える電子マネー入金機からの入金金額データ及び前記復号された利用金額データに基づき、前記ICマネーカードに対する入金と出金との大小関係を比較して入出金の正当性を確認する不正検出手段を有する管理コンピュータと；を備えることによって達成される。

【0011】

【発明の実施の形態】本発明は、従来、企業内等の使用場所が限られたエリア内でセキュリティが確保されて使用していたプリペイドカードを近郊の提携店でも使用できるようにしたものである。提携店側の売上データをセンター側で収集して決済処理などを行うシステムを構築する場合には、提携店側での売上データの改ざんや通信上でのデータ盗取による通信データの改ざんなど、プリペイドカードが使用可能な全てのエリアにおける不正行為を防止し、システムのセキュリティを確保する必要がある。本発明では、ICカードを電子マネーを格納する媒体として使用し、先ず、利用客のICカードに記憶されている第1の暗号キーを基に利用客の支払いデータを暗号化することによって、店側での支払いデータの改ざんを防止する。次に、店側では、客の支払い金額と同額の回収金額のデータに対して店長等の店舗専用のICカードに記憶されている第2の暗号キーを基に暗号化した回収データを作成する。これらの暗号化は、例えばカード所持者により入力される暗証番号を上記の暗号キーとして、ICカードに予め記録されている暗号化プログラムによって行なわれる。そして、暗号化された回収データと支払いデータを1対にして、売上データとして公衆電話回線等の通信回線を通じて管理会社のサーバ（売上回収データ受付サーバ）に電送する。

【0012】ここで、管理会社とは店側への支払いを代行するとともに、金額の追加及び払い戻しが可能なプリペイドカードを利用者に販売し、店独自の特典や広告などの各種サービスを提供する機関であり、銀行とは異なる機関である。管理会社では、電送元の店の番号を基に、別サーバ（電子マネー発行サーバ）に登録されている復号キーを検索し、この復号キーを基に暗号を解いて復号された回収データを得、次いで回収データに含まれ

る利用者のIDコードより、上記の別サーバに登録されている利用者毎の暗号キーを検索してこれを基に支払いデータを復号し、復号された回収データと支払いデータとを請求データとして記憶する。この時点で支払いデータと回収データとが一致することを確認する。これにより、管理会社に電送される際の傍受によってデータが改ざんされて悪用されることを防止している。

【0013】更に、電子マネーIDを付与して利用者カードの入出金のログを記録し、このログデータに基づいてプリペイドカードの販売金額（ICカードに入金された金額）とそのプリペイドカードによって支払われた金額（利用者の利用金額）の大小関係をチェックすることによって、プリペイドカードの改ざんがなされたことがあるかどうか等の総合的なチェックを行う。更に又、提携店へ確認の帳票を送付し、管理会社の集計決済端末は、提携店側での確認がOKであれば、利用者の利用金額（即ち店の請求金額）を店の銀行口座へ振り込む様にしている。このように、本発明では各種の不正のチェックを行うことにより詐欺による電子マネー（ICプリペイドカード）システムの不正使用を防ぐようにしている。

【0014】以下、図面に基づいて本発明の好適な実施の形態について詳細に説明する。図1は本発明の電子マネーシステムの全体構成の一例を示している。図1において、管理会社（プロバイダー）2は、コンビニエンスストア、書店、飲食店等の提携店1（1a, 1b, …）での利用が可能で且つ金額の追加が可能なプリペイドカード（電子マネーカード）5を発行し、提携店1からの売上データを集計して各種不正のチェックを行い、該当店舗への支払い金額を店の銀行口座へ振り込む等のサービスを提供する機関である。本システムの利用者は、管理会社2に加盟している団体（学校や勤め先等：以下「加盟団体」と言う）の一員（学生、従業員等）である。プリペイドカード5は、専用のカードとしても良く、社員カードや会員制カードをプリペイドカード5として使用できるようにしても良い。本例では、暗号化プログラムを記録したICカードを用いており、暗号化のアルゴリズムとしては、DES（data encryption standard）型アルゴリズムを用いている。

【0015】管理会社2が提供する電子マネーシステムは、利用者が所持するプリペイドカード（ICマネーカード：以下、「ICカード」とする）5及び店舗用ICカード6を発行するカード発行機21と、セキュリティ情報（カード所持者のパスワードやICカード5, 6の暗号解読キー等）KW等のデータを記憶／管理する電子マネー発行サーバ22と、ICカード5への入金（電子マネーのチャージ）を行うための電子マネー入金機23と、ICカード5による支払い機能を有する電子マネーPOS端末24と、電子マネー入金機23によりICカ

ード5へ入金された入金データMD及び電子マネーPOS端末24に蓄積された売上データSDを受信して記憶する売上回収データ受付サーバ25と、セキュリティ情報KW、売上データSD及び入金データMDに基づいてデータの改ざん等の不正（カード偽造、POS端末に記憶されているデータの改ざん、伝送データの改ざん等）のチェックをした後、該当店舗への支払い金額を集計して銀行のコンピュータ3に振込データBDを送信し、支払いの処理を行う集計決済端末26とを備えている。

【0016】各提携店1（1a, 1b, …）側に設置される電子マネーPOS端末24は、公衆電話回線7aを介して管理会社2側に設置される売上回収データ受付サーバ25と接続され、所定の場所に設置される電子マネー入金機23とその他の装置（カード発行機21、電子マネー発行サーバ22、売上回収データ受付サーバ25及び集計決済端末26）は専用線7bを介して相互に接続されている。また、必要に応じて専用線7bを介して、給与天引きのデータPDを処理する加盟団体のコンピュータ（パーソナルコンピュータ又は企業等のセンタコンピュータ等）4が専用線7bを介して接続される。この加盟団体のコンピュータ4には、フレキシブルディスク等の記憶媒体を用いてデータを送ることもできる。更に、集計決済端末26は、専用線若しくは公衆回線を用いたネットワーク7cを介して銀行ホストコンピュータ3に接続されている。なお、各提携店1内の既存のPOSレジの売上データRDは、手入力で電子マネーPOS端末24に入力される。以下、本発明に係る電子マネーシステムの主要部の構成例についてそれぞれ説明する。

【0017】図2は電子マネー入金機23の構成の一例を示しており、図3はその外観図を示している。図2において、電子マネー入金機23は、電子マネーに替える紙幣の受入れ及び釣り銭の返却処理をする紙幣入金ユニット232と、ICカードのデータの読み込み及び電子マネーデータ等の書換えを行うためのICカードリーダライタ233と、ガイダンス表示や入金等の操作を行うためのタッチパネルを装着した表示装置234と、電子マネー残高等の明細をジャーナル印字するためのプリンタ235と、店舗案内表示サービス中には選択した店へ無料で電話をして予約等を行うことができ、また操作中に故障が起きた場合などに担当者と連絡をとるための電話機236と、管理会社2側の売上回収データ受付サーバ25とオンライン接続するための通信装置237と、各機器を制御するパソコンから成る制御部231とを備えている。また、電子マネー入金機23は無停電電源装置40を具備しており、各機器は無停電電源装置40を介して電源に接続されている。

【0018】そして、図3に示すように、電子マネー入金機23の筐体の上部には、タッチパネル式の表示部234aが操作性を考慮して所定の傾斜角を成して設けら

れており、また、表示部234aと同様に所定の傾斜角を成して形成されている前面中央部のパネルには、電話機236、紙幣入金部232a、ICカード（電子マネーカード）のカード挿入口233a及びジャーナル出力口235aが設けられている。本例での電子マネー入金機23は、主な機能として、ICカード5への現金支払いによる入金機能、給与天引き支払いによる入金機能、現金による入金データ及び給与引きデータをサーバ（売上回収データ受付サーバ25）へ送信する送信機能、及び残高照会機能を備えている。本例では、ICカード5に入金できる限度額を支払い形態（現金支払い、給与天引き支払い）毎に設定しており、限度額以上の金額は入金できないようにしている。この限度額の情報は、カード発行時にICカード5内に予め書込まれている。利用者のICカード5に入金された入金データMDは、例えばタイマー起動による締め処理で、1日1回又は所定時間毎に分割して売上回収データ受付サーバ25に送信されるようになっている。なお、電子マネー入金機23側では記憶せずに、入金操作が終了した時点で管理会社2側に送信して売上回収データ受付サーバ25に記憶するようにしても良い。或いは、売上回収データ受付サーバ25側からの指令で入金データMDを収集するようにしても良い。

【0019】図4は電子マネーPOS端末24の構成の一例を示しており、図5はその外観図を示している。図4において、電子マネーPOS端末24は、ICカードのデータの読み込み及び電子マネーデータ等の書換え等を行うためのICカードリーダライタ242と、銀行カードやクレジットカード等のキャッシュレスカードのデータの読み書きを行うための磁気カードリーダライタ243と、ファンクションキー、テンキー等から成るキーボード244と、カード所持者が暗証番号の入力を行うためのコードレスタイプ（光通信式）の暗証入力用キーパッド（光通信テンキー）245と、取引内容や操作手順のガイダンス等を表示するための表示装置246と、支払い明細や売上げ明細をジャーナル印字するためのプリンタ247と、売上データ（暗号化した支払いデータ、及び回収データ）を記録するためのディスク装置248と、管理会社2側の売上回収データ受付サーバ25とオンライン接続するための通信装置249と、各機器を制御するパソコンから成る制御部241とを備えている。

【0020】そして、図5に示すように、電子マネーPOS端末24の筐体の上部の前面パネルは所定の傾斜角を成して形成されており、表示部246a、操作部244a、銀行カード等のキャッシュレスカードの読取部243a及び記録媒体の装填部248aが設けられており、筐体の下部の前面パネルには、ICカード（電子マネーカード）のカード挿入口242aが設けられている。そして、筐体の上部後方にはジャーナル出力口247aが設けられ、更にその後方には暗証入力用キーパッ

ド245が装着されている。

【0021】本例での電子マネーPOS端末24は、商店街事務局や地域情報VAN等とのオンラインネットワーク構築により、高度の顧客情報処理サービスの利用をも可能とするオンライン端末であり、主な機能として、ICカードによる支払いデータを暗号化して回収データとともに蓄積する蓄積機能、ICカードの記録エリアに利用履歴（入出金の取引ログ）を書込むログ機能、店舗専用のICカードの暗号化プログラムによって回収データを暗号化し、支払いデータとともに売上データ（請求データ）として管理会社2側のコンピュータ（本例では売上回収データ受付サーバ25）に送信する送信機能を備えている。この他に、提携店舗のサービス情報（割引率等の特典）や運用情報（請求締め日等）を設定する設定機能、売上げ等のジャーナル印刷機能を備えており、更に、プリペイドカード、銀行カード（銀行POS）、クレジットカード及びポイントサービスが行えるサービスカードのカード処理機能を搭載している。

【0022】電子マネーPOS端末24のジャーナルには、利用者に渡される支払い明細の他に、日替集計、プリペイドカード種別の利用件数・金額、販売枚数、売上集計、銀行カード売上集計等が印字される。上記の売上データの送信機能は、店舗専用ICカード6を用いた場合のみ使用できるようになっている。また、蓄積ファイル（売上データ）の記録媒体としては、本例では出し入れ持ち運び可能なリムーバブルディスク（フレキシブルディスク／書換可能光磁気ディスク等）が使用され、何らかの障害で売上データを管理会社2側に送信できない場合は、記録媒体の持ち運びにより店舗側に送ることができるようにしている。売上データの送信は、店舗用ICカード6の所持者（店長等）の指示により、電子マネーPOS端末24から1日1回又は所定の期間毎に行われる。

【0023】上述のような構成において、先ず、電子マネー入金機23の動作例を図6及び図7のフローチャートに沿って説明する。電子マネー入金機23は、待機状態における初期画面として、例えば電子マネーが利用できる店舗の案内画面を表示部234aに表示しており

（ステップS1）、店舗の詳細案内のメニューが選択された場合は、ジャンル別の店舗の一覧を表示し、更に個別店舗が選択されたときには（ステップS2）、個別店舗の案内画面（広告等）を表示をする。そして、個別店舗の案内と共に表示されている電話番号部にタッチされた場合は、当該店舗の電話に自動ダイヤルする。この自動ダイヤル機能は、利用者に対するサービスの一環として設けられたもので、利用者が店に行く場合など、利用者は電話機236により当該店舗の店員と無料で会話することができる（ステップS3）。

【0024】一方、入金のメニューが選択された場合には（ステップS4）、利用者に対してICカードの挿入

を促すガイダンスを表示し、ICカードの挿入待ちとする（ステップS5）。そして、ICカードが挿入されると、ICカードリーダーライタ233によりデータを読み出し、本システムで発行された利用者カードか否かをIDデータにより確認した後、暗証番号の入力を促すガイダンスを表示部234aに表示する（ステップS6）。暗証番号が入力されると、制御部231では、ICカードのデータに含まれる暗証番号と入力された暗証番号とを照合して個人の認証を行い（ステップS7）、認証が取れたのであれば、図10に示すように、現在の電子マネー残高、入金可能な限度額、入金方法の選択メニュー等を表示する（ステップS8）。

【0025】本例では、入金方法として、現金による入金と給与天引きによる入金があり、利用者はいずれかを選択できるようになっている。先ず前者が選択された場合の処理を説明する。上記ステップS8において入金方法として現金による入金が選択され（ステップS9）、貨幣（本例では紙幣）が投入されたのであれば、投入金額を計数して表示し、ICカードに入金する金額を入力する旨の表示をする（ステップS10）。入金する金額が入力されたのであれば、限度額以内か否かを確認した後（ステップS11）、金額の確認メッセージ（入金額、入金後の電子マネー残高、入金後の入金限度額）を表示して利用者に確認する（ステップS12）。ステップS12において取消しの指示がされたのであれば、カードを返却して動作を終了し（ステップS13）、確認OKの指示がされたのであれば、電子マネーIDを採番する。ここで、電子マネーIDは、電子マネーデータを書替える毎に付与される発行の番号であり、例えば、現金／給与天引きの区分、発行機を特定する番号、発行日を示す情報（例えば基準年月日を1日目とした連番）、発行機毎の連続番号等の情報から構成される。本例では、電子マネー入金機23が電子マネー発行機に相当し、電子マネー入金機23によって上記の各情報を更新して入金毎に電子マネーIDを採番する（ステップS14）。

【0026】そして、ICカードの入金エリア内に、何回目の入金を示す回数、電子マネーID、入金金額及び電子マネー残高を取引履歴として記録すると共に、ICカードの限度金残高エリア内の残高（1月の給与からの引落し限度額、1月の現金利用限度額）及び限度額エリア内の入金可能限度額（給与限度額、現金限度額）を更新をする。ここで、利用履歴のエリアは、入金エリア及び出金エリアから成り、それぞれ複数回の取引を記録できるようになっており、サイクリックに使用される（ステップS15）。そして、電子マネーの入金ログデータ（例えば、入金時の日付、利用者ID、電子マネーID及び入金金額）MDを作成し、前述の送信機能により売上回収データ受付サーバ25に送信する。ここでは、入金処理時に送信する場合を例としている。この入

金ログデータMDは売上回収データ受付サーバ25の記憶手段に記憶され、後述する集計決済端末における不正チェック処理（取引の正当性確認処理）において使用される。入金ログデータの送信が完了した後（ステップS16）、投入金額と入金金額とを比較して釣り銭の有無をチェックし、釣り銭がある場合は釣り銭を投出して返却した後、入金された現金を金庫へ収納する（ステップS17）。そして、入金明細のジャーナルを出力すると共に（ステップS18）、カードを投出して返却し（ステップS19）、入金処理を終了する。

【0027】続いて、給与天引きによる入金処理について説明する。なお、現金により入金処理と同一の処理については簡略化して説明する。上記ステップS9において入金方法として給与天引きによる入金が選択されたのであれば、カード所持者により指定された入金金額を入力して限度額以内か否かを確認した後（ステップS20）、金額の確認メッセージを表示し、取消しの指示がされたのであれば、カードを返却して動作を終了し、確認OKの指示がされたのであれば（ステップS21）、電子マネーIDを採番し（ステップS22）、ICカードを更新する（ステップS23）。そして、電子マネーの入金ログデータMDを作成して売上回収データ受付サーバ25に送信し（ステップS24）、ステップS18へ移行して入金明細のジャーナルを出力すると共に、カードを返却し（ステップS19）、入金処理を終了する。

【0028】次に、電子マネーPOS端末24の動作例を図8のフローチャートに沿って説明する。電子マネーPOS端末24は、待機状態における初期画面として、各機能の選択画面が表示されている。ここでは、店舗情報等の設定機能と各種ジャーナルの印刷機能、及びクレジットカード等の一般的なキャッシュレスカードによる支払い処理については説明を省略し、ICカード5による支払い処理と、売上データの送信処理（締め処理）について説明する。まず、支払い処理について説明する。ステップ30において、支払い処理が指示されたのであれば、利用者カードの挿入を促すガイダンスを表示してICカードの挿入待ちとする（ステップS31）。利用者のICカードがカード挿入口233aに挿入されると、電子マネーPOS端末24の制御部241では、ICカードリーダー242によりデータを読み出し（ステップS32）、本システムで発行された利用者カードか否かをIDデータにより確認した後、暗証番号の入力を促すガイダンスを表示部246aに表示する。レジ担当者は暗証入力用キーパッド245をカード所持者に渡して暗証番号を入力してもらう。

【0029】カード所持者により暗証番号が入力されると、制御部241では、ICカード5のデータに含まれる暗証番号と入力された暗証番号とを照合して個人の認証を行い（ステップS33）、個人認証が取れたのであ

れば、支払い金額の入力を促すガイダンスを表示する。レジ担当者により支払い金額（商品の購入金額）が入力されると（ステップS34）、割引率が設定されている場合には割引額を計算し、割引後の支払い金額を算出する。この割引サービスは店舗毎に予め設定されている（ステップS35）。そして、支払い金額とカード残高とを比較して残高不足でないかどうかを確認し（ステップS36）、残高不足でなければ支払い金額を減額してICカードを更新する。その際、入金エリア内の電子マネー残高を更新すると共に、ICカードの出金エリア内に利用履歴（何回目の出金かを示す回数、電子マネーID、利用日時及び利用場所（店舗番号等））を記録する。

【0030】そして、蓄積ファイルに回収データ（利用履歴の各情報、利用者ID等）を登録すると共に（ステップS37）、ICカードに支払いデータを送り、データの暗号化を指示する。ここで、上記の回収データと支払いデータは同一内容であり、上記の利用履歴の各情報及び利用者ID等から構成されている。ICカードに記録されている暗号化プログラムでは、暗証番号により支払いデータをDES型アルゴリズムを用いて暗号化する（ステップS38）。制御部241では、暗号化された支払いデータを読み出し（ステップS39）、図11に示すように、暗号化された支払いデータSD2'を回収データSD1とともに売上データとして蓄積ファイルに記憶すると共に（ステップS40）、支払い明細を作成してプリンタ247によりジャーナル出力し（ステップS41）、支払い処理を終了する。

【0031】続いて、売上データの送信処理について説明する。上記ステップS30において、締め請求指示がされた場合は、店舗用ICカード6の挿入を促すガイダンスを表示部246aに表示する（ステップS51）。店舗用ICカード6が挿入されると、制御部241では、本システムで発行された当該店舗のカードか否かをIDデータにより確認した後、暗証番号の入力を促すガイダンスをする（ステップS52）。そして、入力された暗証番号とICカード6のデータに含まれる暗証番号とを比較して取扱担当者（店舗担当者）の認証を行い（ステップS53）、認証が取れたのであれば、蓄積された回収データを一件単位若しくはブロック単位でICカード6に送り、暗号化を指示する（ステップS54）。ICカードの暗号化プログラムでは、暗証番号により回収データをDES型アルゴリズムを用いて暗号化する。制御部241では、暗号化された回収データを読み出して（ステップS55）蓄積ファイルの回収データを書替える（ステップS56）。そして、通信装置249を介して売上回収データ受付サーバ25とオンライン接続し（ステップS57）、図12に示すように、暗号化された回収データSD1'及び支払いデータSD2'を売上データSDとして送信し、売上回収データ受付サー

10

20

30

40

50

バ25のD/Bに記憶させる(ステップS58)。そして、売上データSDの処理フラグを請求済みとし(ステップS59)、売上データの送信処理を終了する。

【0032】次に、集計決済端末26の動作例を図13及び図14を参照して、図9のフローチャートに沿って説明する。なお、図14(A)及び(B)は、それぞれ売上回収データ受付サーバ25に記憶される売上データSDと入金データMDのファイル構成の一例を示している。

【0033】集計決済端末26では、所定の期間例えば1月毎に店舗への振込みを行うための処理をする。先ず、売上回収データ受付サーバ25から売上回収データSD1'、SD2'を読み出す(ステップS60)。この時点では両データは暗号化されている。そして、電子マネー発行サーバ22より店舗番号毎の復号キー(解除キー)KW1を取出し(ステップS61)、この復号キーKW1により回収データSD1を復号する(ステップS62)。そして、回収データSD1にある該当利用者IDを基に電子マネー発行サーバ22より暗証番号KW2を読み出し(ステップS63)、この暗証番号KW2をキーに支払いデータを復号する(ステップS64)。そして、それぞれのキーにより復号した回収データSD1と支払いデータSD2とを照合して一致するかどうかを確認し(ステップS65)、一致していない場合は、電子マネーカード若しくは店舗側の操作でデータの改ざんなどによる不正が行われたか、或いは他の何らかの原因によりデータの異常が発生したものと判断して異常有りの出力する。この場合は、不一致箇所などを示す詳細出力を基に、問題を調査する(ステップS66)。

【0034】上記ステップS65において、回収データSD1と支払いデータSD2とが一致している場合は、利用者IDと電子マネーIDを基に、売上回収データ受付サーバ25に記憶されている入金データMDを読み出し(ステップS67)、同一電子マネーIDにおいて入金金額と出金金額とを比較して取引の正当性を確認する(ステップS68)。そして、同一電子マネーIDにおいて入金<出金の場合は異常と判断し、ステップS66に移行して異常有りの出力する。一方、上記ステップS68において入金≧出金の場合は正常と判断し(ステップS69)、銀行振込みデータBDを作成し(ステップS70)、店舗への確認用帳票を打ち出して処理を終了する(ステップS71)。なお、銀行への振込みデータBDの送信は確認用帳票による店舗側の確認後行う。また、当該加盟団体へ給与天引きデータを送信する運用としている場合は、給与天引きのデータPDを加盟団体PC4へ送信する。

【0035】なお、上述した実施の形態においては、カード発行機21と電子マネー入金機22を、別の機器として説明したが、同一装置としても良い。また、提携店1と管理会社2との間の通信回線は公衆電話回線に限る

ものではなく、専用線としても良い。

【0036】

【発明の効果】以上に説明したように、本発明によれば、電子マネーPOS端末により利用者がプリペイドICカードを使用する時に利用金額を利用者用のICカードの暗号化プログラムによって暗号化し、さらに店カードを用いて売上げのデータを暗号化し、両者によって暗号化された1対のデータを纏めて管理会社に送り、管理会社側では、それぞれのデータを最初に登録された解除キーを用いて復号して両データの一致を取るとともに入金と出金の大小関係をチェックするようにしているので、カードの偽造/変造、店舗内における売上データの改ざん、伝送時のデータの改ざん等の不正行為に対して安全なプリペイドシステムを提供することができる。

【図面の簡単な説明】

【図1】本発明の電子マネーシステムの全体構成の一例を示すブロック図である。

【図2】電子マネー入金機の構成の一例を示すブロック図である。

【図3】電子マネー入金機の外観構成の一例を示す斜視図である。

【図4】電子マネーPOS端末の構成の一例を示すブロック図である。

【図5】電子マネーPOS端末の外観構成の一例を示す斜視図である。

【図6】電子マネー入金機の動作例を説明するためのフローチャートである。

【図7】図6の分図である。

【図8】電子マネーPOS端末の動作例を説明するためのフローチャートである。

【図9】集計決済端末の動作例を説明するためのフローチャートである。

【図10】電子マネー入金機の表示画面の一例である。

【図11】本発明における不正のチェック方法を説明するための第1の図である。

【図12】本発明における不正のチェック方法を説明するための第2の図である。

【図13】本発明における不正のチェック方法を説明するための第3の図である。

【図14】売上回収データ受付サーバに記憶される売上データ及び入金データのファイル構成の一例を示す図である。

【符号の説明】

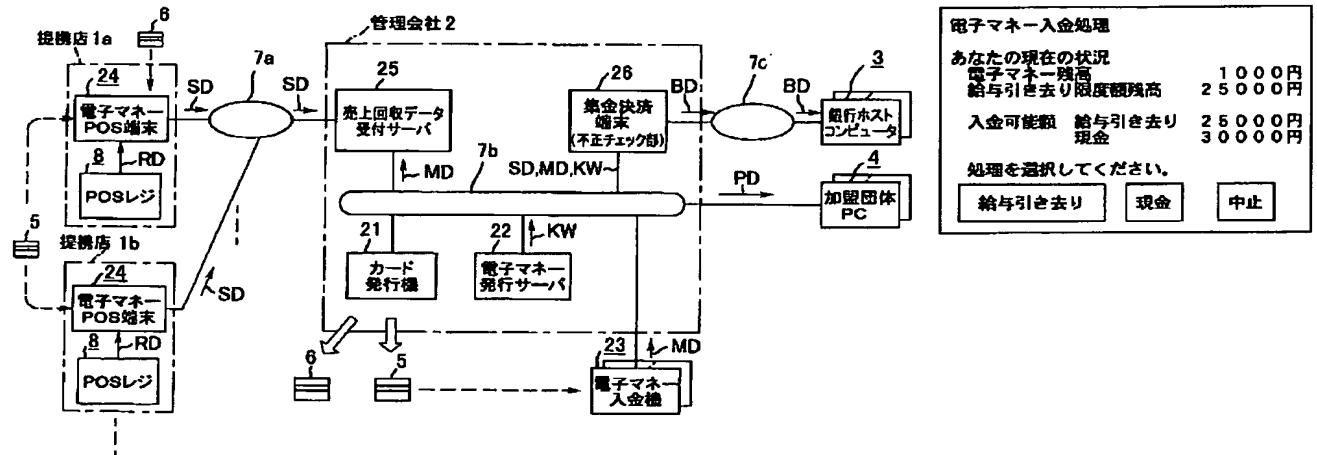
- 1 提携店
- 2 管理会社
- 3 銀行ホストコンピュータ
- 4 加盟団体PC
- 5 プリペイドカード(ICマネーカード)
- 6 店舗用ICカード
- 7 a, 7 b, 7 c 通信回線

- 21 カード発行機 21
 22 電子マネー発行サーバ
 23 電子マネー入金機

- * 24 電子マネーPOS端末
 25 売上回収データ受付サーバ
 * 26 集計決済端末 26

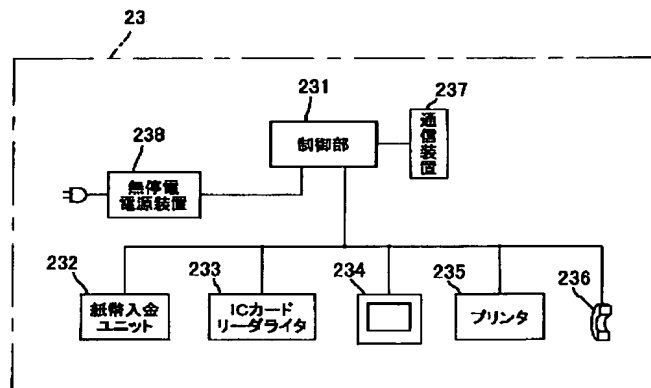
【図1】

【図10】

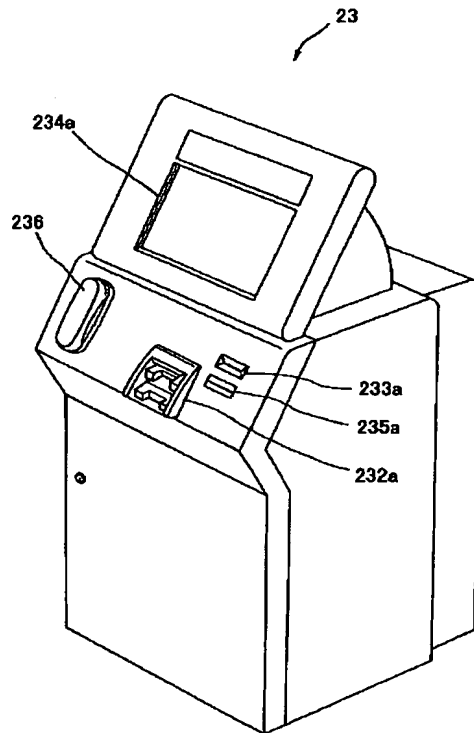
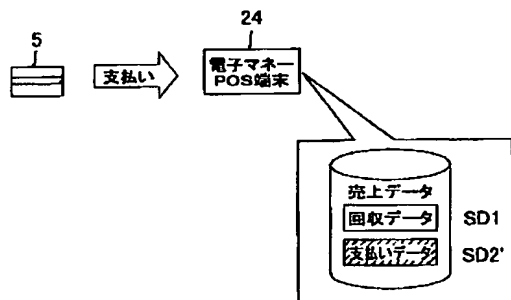


【図2】

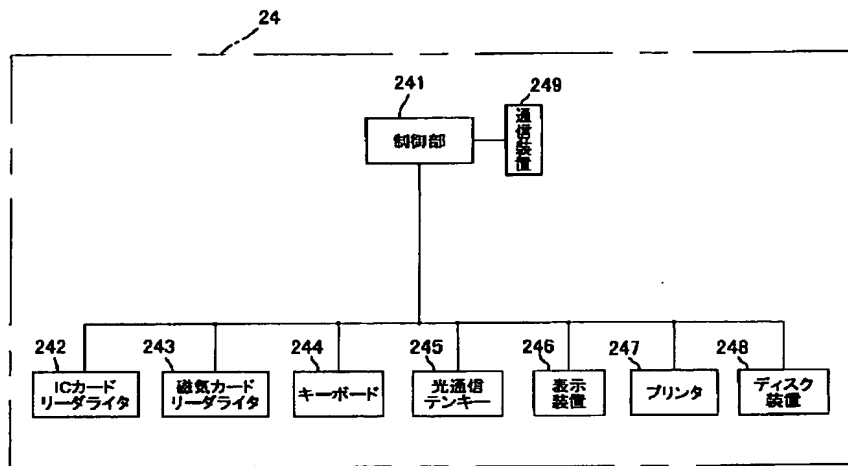
【図3】



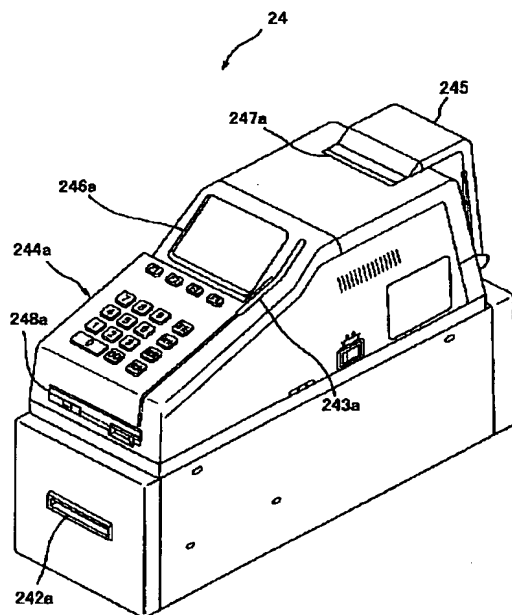
【図11】



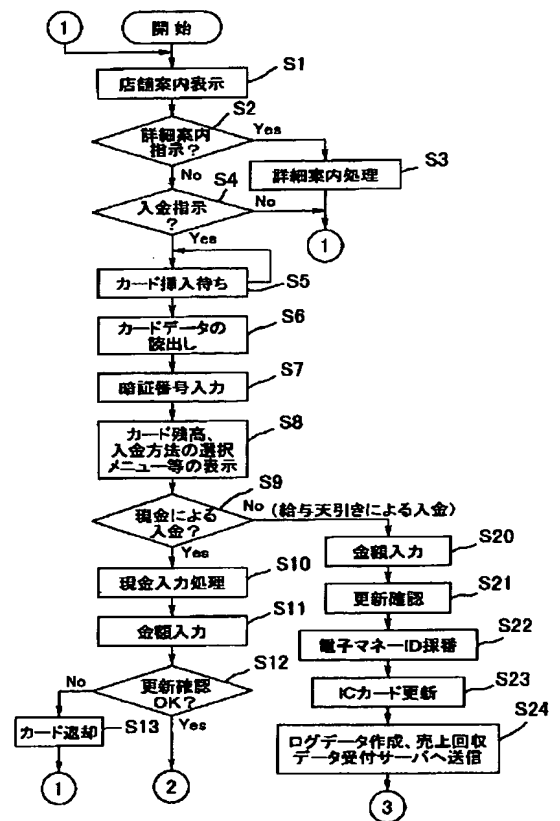
【図4】



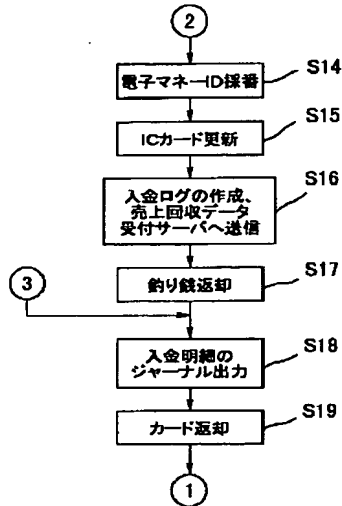
【図5】



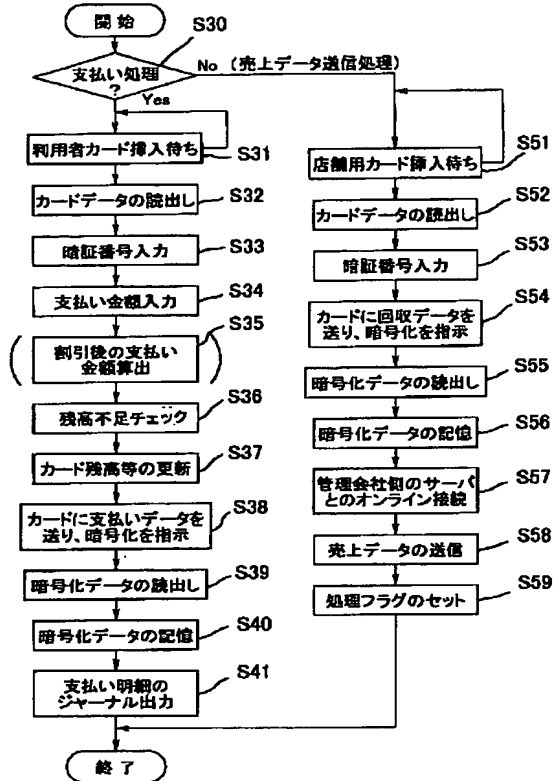
【図6】



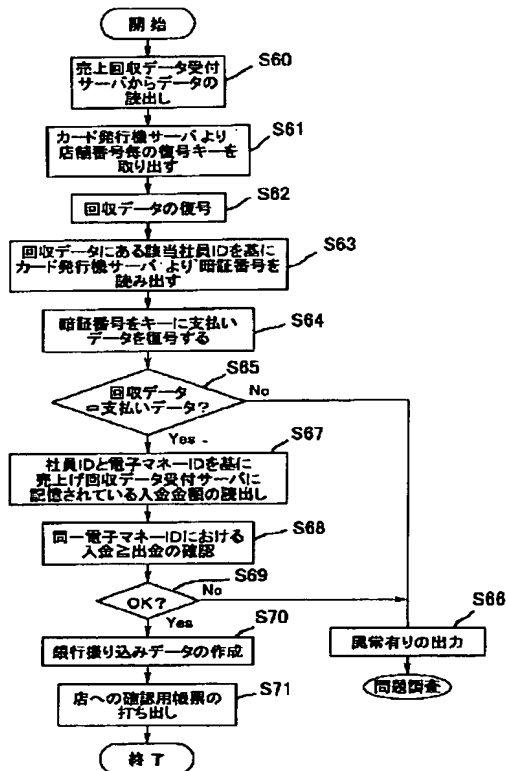
【図7】



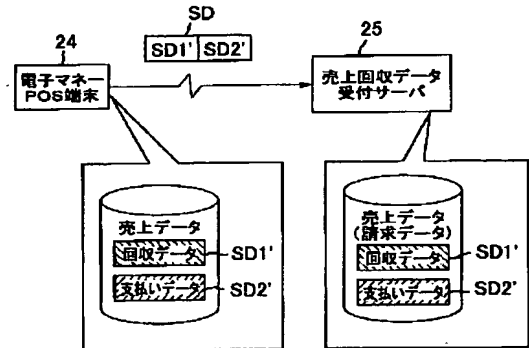
【図8】



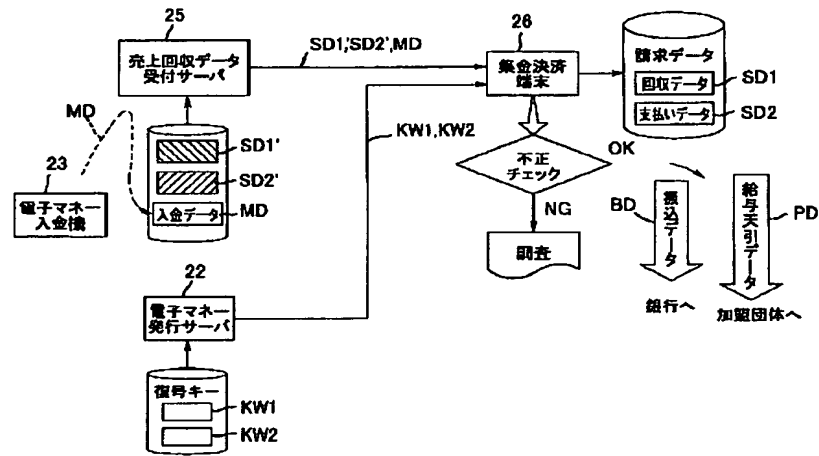
【図9】



【図12】



【図13】



【図14】

SD1	売上上げ日時	利用者ID	電子マネーID	売上げ金額	店舗コード	...
SD(1)						
SD2	購入日時	利用者ID	電子マネーID	購入金額	店舗コード	...
SD(n)						

(A)

MD(1)	入金日時	利用者ID	電子マネーID	金額
MD(m)				

(B)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.